Deutscher Bundestag **Drucksache 18/9267**

18. Wahlperiode 25.07.2016

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Annette Groth, Niema Movassat, Dr. Alexander S. Neu und der Fraktion DIE LINKE.
– Drucksache 18/9117 –

Uploadfilter bei Kriminalämtern und Internetunternehmen für sogenannte extremistische oder radikalisierende Inhalte

Vorbemerkung der Fragesteller

Das internationale „Counter Extremism Project" (CEP) hat eine Software vorgestellt, mit der extremistische Inhalte beim Upload entdeckt werden sollen (Pressemitteilung Counter Extremism Project vom 17. Juni 2016). Das Verfahren basiert auf PhotoDNA, einer Anwendung die von Microsoft ursprünglich für die Bekämpfung von Kinderpornografie entwickelt wurde. Möglich ist die Detektion von Video- und Audioinhalten. Die Erkennungsquote liegt angeblich bei 98 Prozent. PhotoDNA funktioniert nach dem sogenannten Robust Hashing und erstellt einen digitalen Fingerabdruck der Datei. Der Abgleich erfolgt mit einer Hash-Datenbank, die entweder bei den Unternehmen oder auch Behörden geführt wird. Außer Microsoft haben bereits mehrere Internetdienstleister, darunter Facebook, Google, Youtube und Twitter, PhotoDNA auf ihren Servern installiert. Die Firmen scannen dabei auch Inhalte, die von den Nutzerinnen und Nutzern in der privaten Cloud gespeichert werden. Werden dort kinderpornografische Inhalte entdeckt, können die zuständigen Strafverfolgungsbehörden eine Meldung erhalten. Die Fälle werden dann auch international verfolgt, mindestens einmal hat das Bundeskriminalamt (BKA) einen solchen Hinweis von US-Behörden erhalten (golem.de vom 13. Januar 2015). Das BKA hat im Jahr 2012 selbst die Software PhotoDNA zu „Testzwecken" beschafft (Bundestagsdrucksache 17/11299).

Vergangenen Sommer hatte die Europäische Union eine „Meldestelle für Internetinhalte" bei der Polizeiagentur Europol eingerichtet. Strafverfolgungsbehörden und Geheimdienste aus den Mitgliedstaaten der Europäischen Union können dort Inhalte zur Entfernung melden, Europol reicht diese dann an die Internetunternehmen weiter. Die privaten Internetdienstleister haben selbst keinen Zugriff auf die Polizeidaten. Deshalb hat die Europäische Kommission im Dezember 2015 ein „Forum der Internetdienstleister" gestartet, um die Firmen selbst zur Kontrolle des Internets anzuhalten (www.cilip.de vom 19. November 2015). Das „Forum" soll „Instrumente" zur Bekämpfung terroristischer Propaganda im Internet und in den sozialen Medien entwickeln. Ziel ist die Einrichtung einer öffentlich-privaten Datenbank mit bereits gefundenen bzw. entfernten Inhalten. Laut einer Mitteilung der Europäischen Kommission

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 21. Juli 2016 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

(COM(2016) 230 final vom 20. April 2016) arbeiten die Unternehmen „unter voller Einbeziehung von Europol“ an der gemeinsamen Meldeplattform. Dabei kommt vermutlich ebenfalls die von Microsoft entwickelte Software PhotoDNA zur Anwendung. Das Bundesministerium des Innern bestätigt, „die technische Identifizierung gleicher bzw. ähnlicher Internetinhalte“ erfolge anhand von Hashwerten (Bundestagsdrucksache 18/8845). Ein solcher Uploadfilter sei aus Sicht der Bundesregierung „bei den Unternehmen anzusiedeln“. Fraglich ist jedoch, wo die benötigte Datenbank mit Hashwerten von Dateien mit „extremistischen oder terroristischen Inhalten“ geführt wird. Ebenfalls unklar ist, ob dort lediglich solche Internetinhalte gespeichert werden, die bereits einmal hochgeladen wurden, oder ob europäische Kriminalämter (inklusive Europol) dort auch unveröffentlichtes Material zur etwaigen Löschung hinterlegen können.

Im Hinblick auf die sitzungsfreie Zeit des Deutschen Bundestages und die Qualitätssicherung der Antworten erklären sich die Fragesteller mit einer Fristverlängerung für die Bearbeitung der Kleinen Anfrage einverstanden.

Vorbemerkung der Bundesregierung

Die Bundesregierung beantwortet die im Rahmen des parlamentarischen Fragerechts angefragten Sachverhalte gegenüber dem Deutschen Bundestag grundsätzlich transparent und vollständig, um dem verfassungsrechtlich verbrieften Aufklärungs- und Informationsanspruch des Deutschen Bundestages zu entsprechen. Soweit Anfragen Umstände betreffen, die aus Gründen des Staatswohls geheimhaltungsbedürftig sind, hat die Bundesregierung aber zu prüfen, ob und auf welche Weise die Geheimhaltungsbedürftigkeit mit dem parlamentarischen Informationsanspruch in Einklang gebracht werden kann (BVerfGE 124, Seite 161, 189). Evident geheimhaltungsbedürftige Informationen muss die Bundesregierung nach der Rechtsprechung des Bundesverfassungsgerichts nicht offenlegen (BVerfGE 124, 161, 193 f.).

Die Bundesregierung ist nach sorgfältiger Abwägung zu der Auffassung gelangt, dass die Fragen 23, 24 und 25d aus Geheimhaltungsgründen teilweise nicht in dem für die Öffentlichkeit einsehbaren Teil beantwortet werden können.

Zwar ist der parlamentarische Informationsanspruch grundsätzlich auf die Beantwortung gestellter Fragen in der Öffentlichkeit angelegt. Die teilweise Einstufung der Antwort auf die Fragen 23, 24 und 25d als Verschlusssache (VS) mit dem Geheimhaltungsgrad „VS – Nur für den Dienstgebrauch“ ist aber im vorliegenden Fall erforderlich.

Nach § 3 Nummer 4 der Allgemeinen Verwaltungsvorschrift zum materiellen und organisatorischen Schutz von Verschlusssachen (Verschlusssachenanweisung, VSA) sind Informationen, deren Kenntnisnahme durch Unbefugte für die Interessen der Bundesrepublik Deutschland oder eines ihrer Länder nachteilig sein können, entsprechend einzustufen. Eine zur Veröffentlichung bestimmte Antwort der Bundesregierung auf diese Fragen würde spezifische Informationen zur Tätigkeit, insbesondere zur Methodik und den konkreten technischen Fähigkeiten der Sicherheitsbehörden einem nicht eingrenzbaren Personenkreis – auch der Bundesrepublik Deutschland möglicherweise gegnerisch gesinnten Kräften – nicht nur im Inland, sondern auch im Ausland zugänglich machen. Dabei würde die Gefahr entstehen, dass ihre bestehenden oder in der Entwicklung befindlichen operativen Fähigkeiten und Methoden aufgeklärt würden. Dies kann für die wirksame Erfüllung der gesetzlichen Aufgaben der Sicherheitsbehörden und damit für die Interessen der Bundesrepublik Deutschland nachteilig sein. Diese Informationen werden daher gemäß § 3 Nummer 4 VSA als „VS – Nur für den Dienstgebrauch“ eingestuft und dem Deutschen Bundestag gesondert übermittelt.

1. Welchen Inhalt hat nach Kenntnis der Bundesregierung ein „Verhaltenskodex“, den die Europäische Kommission am 31. Mai 2016 vorgestellt hat und der mit den Diensteanbietern Facebook, Twitter, YouTube und Microsoft abgestimmt wurde (Bundestagsdrucksache 18/8845)?

2. Wann und wo soll dieser „Verhaltenskodex“ nach Kenntnis der Bundesregierung veröffentlicht werden?

3. Welche weiteren Beteiligten haben den „Verhaltenskodex“ nach Kenntnis der Bundesregierung unterzeichnet, bzw. was ist hierzu geplant?

4. Auf welche Weise wollen die Unternehmen nach Kenntnis der Bundesregierung „stärker gegen illegale Hassbotschaften auf ihren Plattformen vorgehen“?

Die Fragen 1 bis 4 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der Kodex ist unter der Internet-Adresse http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf öffentlich abrufbar. Darüber hinaus liegen der Bundesregierung keine weiteren Erkennntnisse vor.

5. Auf welche Weise haben welche Bundesbehörden in der Vergangenheit mit dem „Counter Extremism Project” kooperiert oder von dort Analysen erhalten?

In der Vergangenheit fand keine Zusammenarbeit von Bundesbehörden mit dem „Counter Extremism Project“ statt.

6. Was ist der Bundesregierung über Pläne des „Counter Extremism Project” (CEP) bekannt, die Internetanbieter zur Einführung einer Software zu bewegen, mit der extremistische Inhalte beim Upload entdeckt werden sollen?

7. Welche Internetanbieter haben einen solchen Filter nach Kenntnis der Bundesregierung bereits eingeführt?

Die Fragen 6 und 7 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

8. Welche technischen Werkzeuge zur automatisierten Erkennung von extremistischen Inhalten hält das Bundesinnenministerium derzeit für prinzipiell geeignet?

Der Bundesregierung liegen keine vertieften Erkenntnisse hinsichtlich technischer Werkzeuge zur automatisierten Erkennung von extremistischen Inhalten vor. Im Übrigen wird auf die Antwort der Bundesregierung zu Frage 13 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/8845 verwiesen.

9. Auf welche Weise hat das BKA die zu „Testzwecken" beschaffte Software PhotoDNA eingesetzt?

   a) Auf welche Bild- und Videodatenbanken wurde dabei zugegriffen?

   b) Seit wann ist PhotoDNA nach den Tests beim BKA nicht mehr im Einsatz?

Die Software „PhotoDNA" wurde zu Testzwecken beschafft. Die Software selbst wurde jedoch im Bundeskriminalamt (BKA) nicht eingesetzt. Dem Quellcode wurden lediglich einzelne Funktionalitäten zur Ähnlichkeitensuche von Bilddaten entnommen.

10. Inwiefern wird PhotoDNA nach Kenntnis der Bundesregierung auch bei der Polizeiagentur Europol eingesetzt oder getestet bzw. was ist hierzu geplant?

Der Bundesregierung liegen keine Erkenntnisse vor, dass PhotoDNA auch bei der Polizeiagentur Europol eingesetzt oder getestet werden soll bzw. was hierzu geplant ist.

11. Auf welche Gesichtsbilder kann das BKA außer den in INPOL (das beim BKA betriebene elektronische Informationssystem der Polizei) eingestellten, biometrischen Fotos für einen computergestützten Lichtbildvergleich im Einzel- oder im Regelfall zugreifen?

Das BKA besitzt derzeit keine Möglichkeit für einen computergestützten Lichtbildvergleich von über den INPOL-Bestand hinausgehenden digitalen Gesichtsbildern.

12. Was ist der Bundesregierung darüber bekannt, welche Inhalte bzw. Formate mit der Software PhotoDNA erkannt werden können?

Das Programm PhotoDNA wird im BKA nicht als eigenständige Software eingesetzt, sondern findet als Implementierung in forensischen Tools Anwendung. Die Funktionen von PhotoDNA arbeiten hierbei mit robusten Hashalgorithmen, um von dargestellten Bildinhalten eine Art „Fingerabdruck" zu erstellen. Mit diesem lassen sich inhaltsgleiche oder ähnliche Bilder wiedererkennen. Beim eigentlichen Abgleich werden die Hashwerte zweier Bilder verglichen. Bei Gleichheit oder Abweichungen bis zu einem definierten Umfang wird eine Übereinstimmung oder Ähnlichkeit festgestellt.

13. Wie hoch schätzt sie die Erkennungsquote der Anwendung?

Mithilfe der Funktionalitäten von PhotoDNA wird eine Ähnlichkeitssuche durchgeführt. Zu Erkennungsquoten kann keine Aussage getroffen werden.

14. Was ist der Bundesregierung darüber bekannt, auf welche Datenbanken die von einigen Providern bereits eingeführte Software PhotoDNA für den Abgleich zugreift?

Der Bundesregierung liegen keine Erkenntnisse vor.

15. In welchen bzw. wie vielen Fällen haben Bundesbehörden Meldungen ausländischer Strafverfolgungsbehörden erhalten, wonach PhotoDNA Inhalte auch in der privaten Cloud von Beschuldigten aufgespürt hat und erst dies schließlich zu Ermittlungen deutscher Kriminalämter führte?

16. Von welchen konkreten Behörden stammten die Hinweise?

Die Fragen 15 und 16 werden aufgrund des Sachzusammenhangs gemeinsam beantwortet.

Der Bundesregierung liegen keine Erkenntnisse vor.

17. Was ist der Bundesregierung darüber bekannt, in welchen EU-Mitgliedstaaten Meldestellen für extremistisches, terroristisches oder „radikalisierendes“ Material im Internet eingeführt wurden oder werden, und wo sind diese angesiedelt?

Die Bundesregierung besitzt keine Übersicht über nationale Meldestellen von EU-Mitgliedstaaten im Sinne der Fragestellung. Nach Kenntnis der Bundesregierung haben 25 Mitgliedstaaten nationale Kontaktstellen für die „European Union Internet Referral Unit“ (EU IRU) eingerichtet.

18. Was ist der Bundesregierung über technische Aspekte der gemeinsamen Meldeplattform von Europol und den Internetunternehmen bekannt?

Die Bundesregierung hat keine Erkenntnisse über technische Aspekte einer gemeinsamen Meldeplattform von Europol und Internetunternehmen.

19. Inwiefern soll dort zur „Identifizierung gleicher bzw. ähnlicher Internetinhalte“ die Software PhotoDNA zur Anwendung kommen?

Der Bundesregierung liegen hierzu keine Erkenntnisse vor.

20. Welche Haltung vertritt die Bundesregierung zur Frage, ob die gemeinsame Meldestelle Uploads lediglich auf Inhalte überprüft, die bereits einmal hochgeladen wurden, oder ob europäische Kriminalämter (inklusive Europol) dort auch unveröffentlichtes Material zur etwaigen Löschung durch die Internetanbieter hinterlegen können?

Die Bundesregierung hat zu der Frage noch keine Haltung abgestimmt.

21. Was ist der Bundesregierung darüber bekannt, auf welche Weise das britische Projekt „Research, Information and Communications Unit“ (RICU), das dem dortigen Innenministerium untersteht, an EU-Vorhaben zur Entwicklung von „Gegenpropaganda“ beteiligt ist (http://cage.ngo/publication/we-are-completely-independent/)?

Experten der britischen Research, Information and Communications Unit (RICU) tragen zur inhaltlichen Ausgestaltung der Netzwerktreffen des Syria Strategic Communications Advisory Teams (SSCAT), einem von der Europäischen Kommission finanzierten Projekt, bei. Zudem stellen sie ihre Expertise und Beratungsleistung im Rahmen des SSCAT-Projektes den EU-Mitgliedstaaten zur Verfügung.

a) Welche Gruppen der „Zivilgesellschaft“ werden von EU-Projekten, an denen die RICU beteiligt ist, gefördert oder unterstützt?

Hierzu liegen der Bundesregierung keine Erkenntnisse vor.

b) Auf welche Weise haben dem Bundesinnenministerium nachgeordnete Behörden bislang mit der RICU zusammengearbeitet?

Eine institutionalisierte Zusammenarbeit zwischen dem Bundesministerium des Innern nachgeordneten Behörden und RICU findet aktuell nicht statt. Vertreter des BKA sowie der Bundeszentrale für politische Bildung (BpB) haben jedoch durch Teilnahme an den Netzwerktreffen des SSCAT bzw. durch bilaterale Gespräche mit Experten von RICU in Kontakt gestanden.

22. Welchen Inhalt hatte die EMPACT-Maßnahme „Cybercrime – cyber attacks“, die das BKA gemeinsam mit dem spanischen Centro de Inteligencia contra el Terrorismo y el Crimen Organizado (CITCO), der französischen Gendarmerie Nationale, der niederländischen Polizei und dem kroatischen Innenministerium durchführte (www.europol.europa.eu/sites/default/files/publications/empact_01_oap.2015_grants_awarded_0.pdf)?

Bei der in Rede stehenden „EMPACT-Maßnahme“ handelt es sich nach Kenntnis der Bundesregierung um eine durch den „Internal Security Fund“ (ISF) der Europäischen Union geförderte Maßnahme des „operativen Aktionsplans (OAP) Cyber-Attacks 2015“. Informationen zu den Maßnahmen des „OAP Cyber-Attacks 2015“ wurden bereits im Rahmen der Kleinen Anfrage der Fraktion DIE LINKE. zu Kooperationen zwischen der EU und den USA im Bereich Cybersicherheit unter Frage 23 angefragt (Bundestagsdrucksache 18/4074) und beantwortet (Bundestagsdrucksache 18/4286).

23. Welche automatisierte Verfahren zur Auswertung von sozialen Medien bzw. deren Integration in Fall- oder Vorgangsbearbeitungssysteme kommen bei den dem Bundesinnenministerium nachgeordneten Behörden zum Einsatz (heise.de vom 28. Juni 2016)?

Das BKA benutzt Software, deren Funktionalitäten auch zur automatisierten Auswertung in Sozialen Medien geeignet sind. Im Übrigen wird auf den als „VS – Nur für den Dienstgebrauch“ eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

Das Technische Hilfswerk (THW) nutzt für das Monitoring „Echobot Monitoring“ der Echobot Media Technologies GmbH. Zur Verwaltung der verschiedenen Social Media-Auftritte verwendet das THW ein Content-Management-Tool. Hierbei handelt es sich um das Programm „Social Hub“ der maloon GmbH.

24. Welche Marktsichtungen oder Studien hat das Bundesinnenministerium hierzu durchgeführt oder beauftragt?

Durch das Sachgebiet Presse- und Öffentlichkeitsarbeit des THW wurden verschiedene Produkte recherchiert und erfasst (Marktsichtung). Auf dieser Grundlage wurden Angebotsabfragen bei fünf verschiedenen Anbietern durchgeführt und am Ende das wirtschaftlichste Produkt ausgewählt. Eine Studie wurde durch das THW nicht beauftragt.

---

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch“ eingestuft. Die Anlage ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.

Im Übrigen wird auf den als „VS – Nur für den Dienstgebrauch" eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

25. Was ist der Bundesregierung über die Funktionsweise der Software rsNetMAn der Firma rola Security Solutions/T-Systems bekannt?

a) Wie viele Webseiten oder Einträge in sozialen Medien werden laut dem Hersteller für die Analyse in rsNetMAn ausgewertet?

b) Welche weiteren Recherchefunktionen können über rsNetMAn ausgeführt werden (etwa Wildcardsuche, fragmentarische Suche, phonetische Suche, Ähnlichkeitssuche, Komplexrecherche, geobezogene Recherche)?

c) Mit welchen Einschränkungen ist über die Software rsNetMAn auch die Suche nach visuellen Inhalten möglich?

Der Bundesregierung sind folgende Angaben des Herstellers bekannt: Mittels der Software rsNetMAn ist die Analyse von 150 000 000 Webseiten sowie von 500 000 000 Tweets pro Tag möglich. Des Weiteren soll die Software auch die Suche nach visuellen Inhalten ermöglichen. Überdies soll die Analyse über Schlüsselwörter, Metadaten, Geoinformationen (z. B. die Herkunft einer Nachricht) sowie über die verwendeten Bilder (Logos, Symboliken) möglich sein.

Weitere Erkenntnisse zur Funktionsweise der Software rsNetMAn liegen der Bundesregierung nicht vor.

d) Inwiefern wird für den Einsatz von rsNetMAn schon jetzt nach extremistischen, terroristischen oder „radikalisierenden" visuellen Inhalten gesucht?

Es wird auf den als „VS – Nur für den Dienstgebrauch" eingestuften Antwortteil gemäß der Vorbemerkung der Bundesregierung verwiesen.*

* Das Bundesministerium des Innern hat die Antwort als „VS – Nur für den Dienstgebrauch" eingestuft. Die Anlage ist im Parlamentssekretariat des Deutschen Bundestages hinterlegt und kann dort von Berechtigten eingesehen werden.



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333